

REMARKS

Reconsideration and allowance of the above-identified application are respectfully requested. Claims 1-9 remain pending, wherein it is proposed to amend claim 1. Entry of the amendment to claim 1 in the period after a final rejection is appropriate because the amendment addresses an objection to the specification and rejection of the claim under 35 U.S.C. § 112, first paragraph. Accordingly, this amendment does not raise new issues that would require further search and/or examination.

The specification is objected to and claim 1 is rejected under 35 U.S.C. § 112, first paragraph. Claim 1 has been amended to address the objection and rejection. Accordingly, withdrawal of the objection and rejection is respectfully requested.

Claims 1-9 are rejected under 35 U.S.C. §103(a) as unpatentable over European patent document EP 0 944 203 A2 ("Turunen") in view of U.S. Patent No. 6,563,800 to Salo et al. ("Salo") and Mouly et al., "*GSM System for Mobile Communications*" ("Mouly"). This ground of rejection is respectfully traversed.

The combination of Turunen, Salo and Mouly does not render Applicants' claim 1 obvious because the combination does not disclose or suggest all of the elements of Applicants' claim 1. For example, the combination does not disclose or suggest a home authentication, authorization and accounting server (HAAA) and a visitor authenticating authorization and accounting (VAAA) server. The

combination also does not disclose or suggest that “identity information sufficient to enable said VAAA server to communicate with said HAAA server so as to authenticate the proposed connection” is conveyed by user intervention to the VAAA server. Additionally, the combination does not disclose or suggest that “the PIN is encoded and forwarded to the user’s mobile telephone and transferred to the browser to authenticate the requested visiting access to the W-LAN.” Moreover, the combination does not disclose or suggest that “the cost of such access is billed to the user’s cellular mobile account.”

Turunen discloses a system for mobile internet access that allows a mobile internet-access host 9 to roam from a local area network 3 to a GSM network 6 or “Hot spot LAN” 7 or 8. When mobile host 9 roams, it deregisters from local area network 3 and registers with GSM network 6. The local area network’s home agent HA sends an internet security key via GSM Short Message Service (SMS) to mobile terminal 9. *Mobile terminal 9 then sends its new address with authentication data generated using the security key to the home agent HA.*

The Office Action states that the foreign agent FA of Turunen corresponds to the visitor authentication, authorization and accounting (VAAA) server of Applicants’ claim 1, and that the home agent HA of Turunen corresponds to the home authentication, authorization and accounting (HAAA) server of Applicants’ claim 1. However, Turunen is completely silent on either the home agent HA or foreign agent FA having any type of accounting function. Accordingly, the home agent HA of Turunen cannot correspond to the HAAA of Applicants’ claim 1 and

the foreign agent FA of Turunen cannot correspond to the FAAA of Applicants' claim 1.

Regarding conveying to the VAAA server by user intervention identity information, the Office Action states that a user moving the mobile host to a foreign network corresponds to the user intervention. However, Applicants' claim 1 recites that the identity information is conveyed "by user intervention" and not merely that after a user moves a mobile host that the host automatically sends information to its home agent HA as disclosed by Turunen.

Additionally, Turunen discloses that mobile terminal 9 receives the internet security key from the home agent and an internet address from the foreign agent. *Mobile terminal 9 then sends* this internet address with authentication data *to the home agent HA* of local area network 3. In contrast, Applicants' claim 1 recites that the "identity information sufficient to enable said VAAA server to communicate with said HAAA server so as to authenticate the proposed connection". There is no disclosure or suggestion in Turunen of the foreign agent FA being enabled by the received identity information to communicate with the home agent HA as would be required to reject Applicants' claim 1 under the reasoning provided by the Office Action.

Moreover, Turunen does not disclose or suggest that the PIN forwarded to "the user's mobile telephone [is] transferred to the browser to authenticate the requested visiting *access to the W-LAN.*" Instead, in Turunen mobile terminal 9

sends authentication data, derived from the internet security key, to the home agent HA. Turunen does not disclose or suggest that the internet security key, or the authentication data derived from the key, is used by a browser to “authenticate the requested visiting *access to the W-LAN*.” In other words, Turunen does not disclose or suggest that the internet security key or anything derived from the key is used for authenticating *access to the first W-LAN*.

Turunen also does not disclose or suggest that “the cost of such access is billed to the user’s cellular mobile account.” Turunen is completely silent on billing for access, and accordingly, cannot disclose or suggest billing such access to a cellular mobile account.

Salo does not remedy any of the above-identified deficiencies of Turunen with respect to Applicants’ claim 1. Salo discloses a system for a remote access device to obtain data from a data center. Referring now to Figure 2 of Salo, a subscriber inputs an address of an enterprise network into a browser, and the user is prompted by a login server (LS) 142 for login credentials and a personal identification number (PIN). When the proper credentials and PIN are input by the user, the user is provided access to data from the data center. However, Salo, like Turunen, is completely silent on accounting functions. Accordingly, Salo cannot disclose or suggest a visitor authentication, authorization and accounting (VAAA) server or home authentication, authorization and accounting (HAAA) server as recited in Applicants’ claim 1. Moreover, Salo cannot disclose

or suggest that “the cost of such access is billed to the user’s cellular mobile account.”

Additionally, Salo does not disclose or suggest conveying identity information to a VAAA server as a result of user intervention or a VAAA server communicating with an HAAA server to authenticate the proposed connection as recited in Applicants’ claim 1.

Regarding the use of the PIN, Salo discloses that this is used for authenticating with the data center, and not “to authenticate the requested visiting *access to the W-LAN*” as recited in Applicants’ claim 1.

Mouly provides a general description of the GSM network. However, Mouly does not disclose or suggest “a visitor authentication, authorization and accounting (VAAA) server or home authentication, authorization and accounting (HAAA) server”, a VAAA server communicating with an HAAA server to authenticate the proposed connection, or that a PIN is used “to authenticate the requested visiting *access to the W-LAN*” as recited in Applicants’ claim 1.

The Office Action relies upon Mouly for the disclosure of management standards for GSM networks. The Office Action concludes that “a user employing the GSM network for internet access would be billed for the services he consumes, and that the billing would be applied to the account he uses to obtain such services.” This statement demonstrates that the application of Mouly in the rejection of Applicants’ claim 1 is based upon a misinterpretation of

the plain language of the claim. In particular, Applicants' claim 1 specifically recites that the PIN is "transferred to the browser to authenticate the requested visiting *access to the W-LAN.*" Mouly is directed to a GSM network, and is completely silent on providing *access to a W-LAN.* Accordingly, Mouly and the Office Action have not provided any disclosure or suggestion of billing a user' cellular mobile account for "requested visiting access to" a wireless LAN as recited in Applicants' claim 1.

Because Turunen, Salo and Mouly all do not disclose or suggest "identity information sufficient to enable said VAAA server to communicate with said HAAA server so as to authenticate the proposed connection" is conveyed by user intervention to the VAAA server, that "the PIN is encoded and forwarded to the user's mobile telephone and transferred to the browser to authenticate the requested visiting access to the W-LAN," and that "the cost of such access is billed to the user's cellular mobile account" as recited in Applicants' claim 1, the combination cannot render Applicants' claim 1 unpatentable.

Claims 2, 4, 8 and 9 all variously depend from Applicants' claim 1, and accordingly, are not obvious in view of the combination of Turunen, Salo and Mouly for at least those reasons stated above with regard to claim 1.

The combination of Turunen, Salo and Mouly does not render Applicants' claim 3 obvious because the combination does not disclose or suggest "the portable computing device is coupled to the mobile telephone, and the transfer of

the PIN to the browser is effected automatically by means including software supported by the portable computing device”.

Instead of providing a prior art reference disclosing or suggesting the elements of claim 3, the Office Action cites *In re Venner*, 262 F.2d 91, 95 (CCPA 1958) for the proposition that automating an manual activity is obvious. As discussed in M.P.E.P. § § 2144 and 2144.04, the examiner may rely upon legal precedent when “the *facts* in a prior legal decision *are sufficiently similar* to those in an application under examination.” (emphasis added). *In re Venner* is directed to a permanent mold casting apparatus that the court held broadly provides “an automatic or mechanical means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art.” (M.P.E.P. § 2144.04 III.). Because *In re Venner* is directed to a permanent mold casting apparatus and not an access authentication system as recited in Applicants’ claim 3, the facts of *In re Venner* are not sufficiently similar to those of the claims currently being examined. Additionally, unlike the claims in *In re Venner* that “broadly” provided an automatic means to replace a manual activity, Applicants’ claim 3 recites particular structure, such as including software supported by the portable computing device, that transfers the PIN, thereby further highlighting the inapplicability of *In re Venner* to the claims currently under examination.

Because the case law relied upon by the Office Action is not applicable to the facts claim 3, and because the Office Action has not provided a prior art reference that discloses or suggests all of the elements of this claim, the Office

Action has not provided enough information to establish a *prima facie* case of obviousness with respect to claim 3.

The combination of Turunen, Salo and Mouly does not render Applicants' claim 5 obvious because the combination does not disclose or suggest "the user employs the browser to convey said identity information, via the first W-LAN, to the VAAA." To reject claim 5 the Office Action cites sending a care-of-address from a mobile host to the host's home network disclosed in col. 3, lines 50-55 of Turunen, and the use of a web browser to send a PIN to a login server disclosed in col. 9, lines 4-17 of Salo. However, the care-of-address of Turunen and the PIN of Salo serve completely different purposes and, therefore, cannot be identified as the same element. While the care-of-address of Turunen is sent to the home network in order to enable the home network to redirect datagrams to that new care-of-address, the PIN of Salo is used to authenticate the access to the remote access device. Accordingly, it appears that the rejection of claim 5 is based upon improper hindsight reconstruction in which various elements of Turunen and Salo are selected for the sole purpose of rejecting Applicants' claim 5, and not because one skilled in the art would have considered the combination of such elements obvious.

The combination of Turunen, Salo and Mouly does not render Applicants' claims 6 and 7 obvious because the combination does not disclose or suggest that "the PIN is combined with masking information" as recited in claim 6 or that "said masking information is randomly derived" as recited in claim 7. The Office

Action relies upon the GSM encryption as corresponding to the masking information recited in Applicants' claims 6 and 7. However, a mere encoding of an authentication key cannot be regarded as a combination with masking information, but instead, the authentication key of Turunen is transmitted as such.


For at least those reasons stated above, it is respectfully requested that the rejection of claims 1-9 as being obvious in view of the combination of Turunen, Salo and Mouly be withdrawn.

In light of the foregoing remarks, this application should be in condition for allowance, and early passage of this case to issue is respectfully requested. If there are any questions regarding this amendment or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket #3036/50289).

Respectfully submitted,

April 5, 2006



Stephen W. Palan
Registration No. 43,420

CROWELL & MORING LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
SWP

2746356v1